UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,690	02/03/2005	Kazunori Saito	1560-0422PUS1	8523

2292 7590 02/22/2010

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
SCHWARTZ, DARREN B	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
02/22/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/523,690	SAITO, KAZUNORI	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2010 and 04 February 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7,8 and 11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,7,8 and 11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Applicant amends claims 1-3, 7 & 8 and claims 4, 5, 9 & 10 have been cancelled. Claims 1-3, 7, 8 & 11 are presented for examination.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04 February 2010 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 1-3, 7, 8 and 11 have been considered but are moot in view of the new grounds of rejection. However, the Examiner remarks on the amendments filed.

1. Applicant claims the following limitation: "if the read input data is a branch instruction, determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read and if the branch destination address is larger than the branch origin address storing the branch destination address and branch origin address" (emphasis added).

The Examiner applies Hollander et al (U.S. Pat 6301699 B1), hereinafter referred to as Hollander. Hollander teaches, *at least*, in Figure 7, elements 141 & 142,

"ANALYZE NEXT INSTRUCTION," "TYPE OF INSTRUCTION." The Examiner further notes 2 of the 3 options provided by element 142 are "TARGET OF A JUMP" & "ELSE" which represent alternatives to the "TYPE OF INSTRUCTION" jump option. Ergo, Hollander teaches when the "read input data is **not** a branch instruction."

The "if" conditional, by its very nature, exhibits alternative steps in the event the "if" conditional fails; the alternative step(s) may, or may not, be limited to not performing any step(s). While the claimed limitation does not rise to the level of indefiniteness, the claimed limitation is optional.

The prior art meets the optional component of the claim by explicitly teaching, either explicitly or inherently, the conditions to the optional component explicitly fails.

2. Applicant claims "determining whether or not there is a call instruction at the branch destination address, and storing a call destination address of the call instruction if the instruction code at the branch destination address is a call instruction."

A broad and reasonable interpretation of a "call instruction" is inclusive of a "jump instruction" (e.g. jmp). The claim has been analyzed and given its broadest reasonable interpretation in light of and consistent with the written description (*In re Morris*, 127 F.3d 1048, 1053-54, 44 USPQ2d 1023, 1027 (Fed. Cir. 1997)).

The Examiner applies Hollander et al (U.S. Pat 6301699 B1), hereinafter referred to as Hollander. Hollander teaches, *at least*, the following method elements applied in Figure 7, elements 140 → 141 → 142 — "TARGET OF A JUMP" → 146 → 148 → 141

→ 142 — "JUMP INSTRUCTION" → 144. Therefore, Hollander meets the claimed condition in the affirmative and negative.

3. Applicant claims "if the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process."

The Examiner applies Yoshimi (U.S. Pat App Pub 2001/0011346 A1), hereinafter referred to as Yoshimi. Yoshimi teaches, *at least*, in the bottom part of Figure 3 and ¶172-¶173 the "stored call destination address is **not** between the branch origin address and the branch destination address."

The "if" conditional, by its very nature, exhibits alternative steps in the event the "if" conditional fails; the alternative step(s) may, or may not, be limited to not performing any step(s). While the claimed limitation does not rise to the level of indefiniteness, the claimed limitation is optional.

The prior art meets the optional component of the claim by explicitly teaching, either explicitly or inherently, the conditions to the optional component explicitly fails.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 3 recites the limitation "the instruction code group." There is insufficient antecedent basis for this limitation in the claim.

7Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-3, 7, 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hollander et al (U.S. Pat 6301699 B1), hereinafter referred to as Hollander, in view of Yoshimi (U.S. Pat App Pub 2001/0011346 A1), hereinafter referred to as Yoshimi.

Re claims 1, 2, 7 and 8: Hollander teaches a data processing method including receiving input data containing a plurality of instructions codes, and judging whether or not a process executed based on the instruction codes contained in the received data is a malicious process, said method comprising:

sequentially reading instructions of the input data at a time (Fig 7, elt 141; col 8, lines 18-21);

determining whether or not the read data is a branch instruction (Fig 7, elt 141; col 8, lines 18-21);

if the read input data is a branch instruction, determining whether a branch destination address of the branch instruction is larger than a branch origin address based only on the one byte of the data read and if the branch destination address is larger than the branch origin address storing the branch destination address and branch origin address (Figure 7, elements 141 & 142, "ANALYZE NEXT INSTRUCTION," "TYPE OF INSTRUCTION." The Examiner further notes 2 of the 3 options provided by element 142 are "TARGET OF A JUMP" & "ELSE" which represent alternatives to the "TYPE OF INSTRUCTION" jump option).

determining whether or not there is a call instruction at the branch destination address, and storing a call destination address of the call instruction if the instruction code at the branch destination address is a call instruction (Figure 7, elements 140 → 141 → 142 — "TARGET OF A JUMP" → 146 → 148 → 141 → 142 — "JUMP INSTRUCTION" → 144).

However, Hollander does not expressly disclose sequentially reading one byte of the input data at a time; determining whether or not the stored call destination address is between the branch origin address and the branch destination address; if the stored call destination address is between the branch origin address and the branch destination address concluding that the input data includes a malicious process.

Yet, Yoshimi teaches sequentially reading one byte of the input data at a time (Fig 3; ¶20; ¶23; ¶30); determining whether or not the stored call destination address is between the branch origin address and the branch destination address (¶167; ¶172-¶173); if the stored call destination address is between the branch origin address and

the branch destination address concluding that the input data includes a malicious process (Fig 14; ¶158; ¶170-¶176; ¶184).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Hollander with the teachings of Yoshimi, for the purpose of predicting program execution in file processes and judging program execution prior to its execution (¶282).

Re claim 3: The combination of Hollander and Yoshimi teaches means for judging whether or not a predetermined character string is associated with a return address of the instruction (Hollander: Fig 4B, all elts).

Re claim 11: The combination of Hollander and Yoshimi teaches the malicious process causes an erroneous operation in the process executed based on the instruction codes contained in the received data (Hollander: Fig 4b, elt 106: col 4, lines 62-65).

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed

invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTOL-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435